Amendment After Final
U.S. Application No. 10/510,498

Atty. Docket No.: 4020-3
Art Unit No.: 2617

REMARKS/ARGUMENTS

Favorable reconsideration and allowance of the present application are requested in view of the following remarks.

§102 REJECTION – HAVERINEN ET AL

In numbered paragraphs 4-5 (pages 3-10) of the Final Office Action, claims 1-5, 7-13, 15-22 and 24-25 stand rejected under 35 U.S.C. §102(b) as allegedly being anticipated by Haverinen et al. (U.S. Publication 2002/0012433). The present application is a national stage application of an international application PCT/EP02/04865 with an international filing date of May 1, 2002, which is the effective filing date. Thus, Haverinen et al. at best qualifies as a 102(e) prior art. Accordingly, Applicants will treat the above claims as being rejected under 35 U.S.C. §102(e). Applicants respectfully traverse.

For a §102 rejection to be proper, the cited reference must teach or suggest each and every claimed element. *See M.P.E.P. 2131; M.P.E.P. 706.02.* Thus, if the cited reference fails to teach or suggest one or more elements, then the rejection is improper and must be withdrawn.

Independent claim 1 recites "carrying out a challenge-response authentication procedure between the wireless terminal and the public land mobile network through the Access Controller, the wireless terminal provided with a SIM card and adapted for reading data thereof; the method characterized in that the challenge-response authentication submissions in step (c) takes place before having provided an IP connectivity to the user" and "offering the IP connectivity to the user at the wireless terminal, by sending an assigned IP address." As recited, the wireless terminal is first authenticated, and then the IP connectivity is provided.

Amendment After Final
U.S. Application No. 10/510,498

Atty. Docket No.: 4020-3
Art Unit No.: 2617

In a previous Amendment filed on November 23, 2007, Applicants demonstrated that at best, Haverinen et al. discloses allocating the IP address prior to authenticating the mobile terminal with the underlying mobile network. Claim 1, in contrast, recites that the IP address is sent to the wireless terminal after a successful authentication. Accordingly, independent claim 1 is distinguishable over Haverinen et al. *See previous Amendment, page 17, line 14 – page 18, line 12.* For similar reasons, claim 15 was also demonstrated to be distinguishable. *See previous Amendment, page 18, lines 13 – 22.*

The Examiner simply responds by alleging, without support, that Haverinen et al. does not disclose allocating IP address prior to authentication. The Examiner further alleges that it is common knowledge that authentication always takes place before any device is connected to a network and refers to Svensson (US Publication 2003/0120920), paragraphs [0025] and [0026] for support. *See Final Office Action, page 2, numbered paragraph 3.*

First, Applicants note that Svensson is not relied upon in the rejection. If the Examiner wishes to rely upon the teachings of Svensson, then the rejection should properly be under §103 and the Examiner is requested to demonstrate the combinability of Svensson with Haverinen et al. Even assuming that Svensson is combinable, the relied upon paragraphs do not correct the deficiencies of Haverinen et al. Svensson merely discloses authenticating a non-provisioned device 18 to a network using a provisioned device 12. The non-provisioned device 18 communicates with a WLAN 20 across an IEEE 802.11(b) interface and communicates with the provisioned device 12 across a BLUETOOTH interface. Svensson is silent regarding whether IP addresses are allocated after the authentication.

Amendment After Final
U.S. Application No. 10/510,498

Atty. Docket No.: 4020-3
Art Unit No.: 2617

Second, contrary to the Examiner's allegation, Haverinen et al. does not disclose, as claim 1 presently recites, that the challenge-response authentication submissions in the method step c) take place before having provided IP connectivity to the user, and are carried:

- on top of a Point-to-Point layer 2 protocol (such as a Point-to-Point Protocol over Ethernet, generally known as PPPoE) between the wireless terminal and the Access Controller; and

- on an authentication protocol residing at application layer between the public land mobile network and the Access Controller.

In fact, the references made by the Examiner to **Abstract** and paragraphs **[0014]-[0029]** describe a particular challenge authentication procedure between the wireless terminal and the public land mobile network and neither anticipate authentication submission taking place before having provided IP connectivity to the user, nor anticipate two different protocols involved in the transaction, namely a Point-to-Point layer 2 protocol (PPPoE) between the wireless terminal and the Access Controller and an authentication protocol residing at application layer between the public land mobile network and the Access Controller.

Moreover, the references made by the Examiner to paragraph **[0343]** may only be understood in the context of paragraphs [0342]-[0346] with due regard to Fig. 16, in which Haverinen et al. teaches an authentication procedure carried out with an Extensible Authentication Protocol (hereinafter EAP), which is a Point-to-Point Protocol (hereinafter PPP), so that authentication data are exchanged between the wireless terminal (MT) and the public land mobile network (HAAA) via the Access Controller (PAC), wherein the PAC does not know details of the authentication. Fig. 16 illustrates an embodiment of Haverinen et al. whereby the EAP protocol is used for exchanging authentication data between the wireless terminal (MT) and

Amendment After Final
U.S. Application No. 10/510,498

Atty. Docket No.: 4020-3
Art Unit No.: 2617

the Access Controller (PAC), and an EAP over RADIUS protocol is used for exchanging

authentication data between the Access Controller (PAC) and the public land mobile network

(HAAA).

However, in contrast as recited in claim 1, the authentication submissions are carried out

on top of a Point-to-Point layer 2 protocol (PPPoE) between the wireless terminal and the Access

Controller; and on an authentication protocol residing at application layer between the public

land mobile network and the Access Controller. *See also Fig. 3 of the present application for a*

non-limiting illustration.

Even if the Examiner reads on the EAP over RADIUS protocol of Haverinen et al., for

exchanging authentication data between the Access Controller (PAC) and the public land mobile

network (HAAA), the authentication protocol residing at application layer between the public

land mobile network and the Access Controller, (*again see Fig. 3 for non-limiting illustration*)

there is no further passage in Haverinen et al. where one of ordinary skill may learn

authentication submissions carried out on top of a Point-to-Point layer 2 protocol (PPPoE)

between the wireless terminal and the Access Controller. Basically, because a Point-to-Point

layer 2 protocol (PPPoE) is neither the EAP protocol in Haverinen et al. nor cited at all therein

and, more specifically, because the claimed invention features the use of an exemplary EAP on

top of a Point-to-Point layer 2 protocol (PPPoE), embodiment which is neither described nor

suggested nor derivable from Haverinen et al., claim 1 is distinguishable.

Furthermore, as already explained above, the references made by the Examiner to

paragraphs [0014]-[0029] and [0343] describe a particular challenge authentication procedure

between the wireless terminal and the public land mobile network and the EAP protocol used for

authentication already discussed. This teaching in Haverinen et al. does not anticipate the step of

offering IP connectivity to the user at the wireless terminal, by sending an assigned IP address

and other network configuration parameters, once said user has been validly authenticated by the

public land mobile network as recited in claim 1. In fact, there is no reference at all to IP

connectivity in these paragraphs, on whether before or after carrying out the authentication

procedure, and therefore the argument made by the Examiner in this respect is not supported by

Haverinen et al.

Haverinen et al. states on paragraph [0263] that Fig. 9 shows the major signaling steps of

the system of Fig. 7-8, and discloses a first step 301 of allocating and IP address to the Mobile

Terminal (MT) followed by a number of subsequent steps to authenticate the MT to a public

access controller (PAC). The sequence of actions in the process of authenticating the MT is

illustrated in Fig. 9 and detailed in following paragraphs: in [0265] the MT obtaining an IP

address, and in [0266]-[0279] carrying out the authentication procedure.

Consequently, Haverinen et al. does not disclose the above features of carrying out

challenge-response authentication submissions before having provided IP connectivity to the

user, said submissions carried out on top of a Point-to-Point layer 2 protocol (PPPoE) between

the wireless terminal and the Access Controller, and on an authentication protocol residing at

application layer between the public land mobile network and the Access Controller, and

Haverinen et al. does not disclose the above features of offering IP connectivity to the user, by

sending an assigned IP address, once said user has been validly authenticated. Indeed,

Haverinen et al. shows directly the opposite.

Thus, Haverinen et al. fail to solve the problem of lack of security caused by assigning an

IP address to the wireless terminal in clear form before getting an agreement on applicable

ciphering keys, which are obtained while running the authentication process, in order to avoid

Amendment After Final
U.S. Application No. 10/510,498

Atty. Docket No.: 4020-3
Art Unit No.: 2617

that a malicious user might initiate well-known attacks by spoofing this IP address, as described on paragraph [0024] (among other places) of the present application.

The claimed features allow an authentication procedure being carried out before offering IP Connectivity to the user, whereas in Haverinen et al. the authentication is carried out over an Internet Protocol (IP) or over an Extensible Authentication Protocol (EAP), without any indication or suggestion of combining both protocols for different purposes. Moreover, there is nothing in Haverinen et al. that suggests the use of EAP prior to offering IP connectivity to the user. The sequence of actions disclosed by Haverinen et al. in the process of authenticating the MT as illustrated in Fig. 9 clearly start with the MT obtaining an IP address in [0265], and then carrying out the authentication procedure in [0266]-[0279].

Still further, Haverinen et al. does not anticipates the Access Controller of claim 15 comprising a Point-to-Point layer 2 protocol (PPPoE) server for communicating with the wireless terminal, which is arranged for tunneling the challenge-response authentication procedure, and an authentication protocol residing at an OSI application layer for communicating with the public land mobile network.

For at least the reasons stated above, independent claim 15 is distinguishable over Haverinen et al. Claims 2-5, 7-13, 16-22 and 24-25 depend from independent claims 1 or 15 and recite further distinguishing features. Accordingly, these dependent claims are distinguishable over Haverinen et al. Applicants respectfully request that the rejection of claims under §102(e) based on Haverinen et al. be withdrawn.

Amendment After Final
U.S. Application No. 10/510,498

Atty. Docket No.: 4020-3
Art Unit No.: 2617

§103 REJECTION – HAVERINEN ET AL., FINK ET AL.

In numbered paragraphs 6-7 (pages 10-11), claim 6 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Haverinen et al. in view of Fink et al. (US Patent 7,043,633). Applicants respectfully traverse.

Claim 6 depends from independent claim 1, which is demonstrated to be distinguishable over Haverinen et al. Fink et al. does not correct at least the above-noted deficiencies of Haverinen et al. Therefore, claim 1 is distinguishable over the combination of Haverinen et al. and Fink et al. Claim 6 recites further distinguishing features. For at least these reasons, claim 6 is also distinguishable over the combination of Haverinen et al. and Fink et al.

Applicants respectfully request that the rejection of claim 6 based on Haverinen et al. and Fink et al. be withdrawn.

§103 REJECTION – HAVERINEN ET AL., AMIN ET AL.

In numbered paragraph 8 (page 11), claims 14 and 23 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Haverinen et al. in view of Amin et al. (US Patent 6,854,014). Applicants respectfully traverse.

Claims 14 and 23 depend from independent claims 1 and 15, respectively, which are demonstrated to be distinguishable over Haverinen et al. Fink et al. does not correct at least the above-noted deficiencies of Haverinen et al. Therefore, claims 1 and 15 are distinguishable over the combination of Haverinen et al. and Amin et al. Claims 14 and 23 recite further distinguishing features. For at least these reasons, claims 14 and 23 are also distinguishable over the combination of Haverinen et al. and Amin et al.

Amendment After Final
U.S. Application No. 10/510,498

Atty. Docket No.: 4020-3
Art Unit No.: 2617

Applicants respectfully request that the rejection of claims 14 and 23 based on Haverinen et al. and Amin et al. be withdrawn.

CONCLUSION

The application is in condition for allowance. An early notice to that effect is earnestly solicited.

Applicants believe that no fee is required for consideration of this Response. However, should the U.S. Patent and Trademark Office determine otherwise, authorization is hereby granted to charge any fee deficiency, or credit any payment, to our Deposit Account No. 14-1140 referencing docket number 4020-3.

In view of the foregoing and other considerations, all claims are deemed in condition for allowance. A formal indication of allowability is earnestly solicited.

The Commissioner is authorized to charge the undersigned's deposit account #14-1140 in whatever amount is necessary for entry of these papers and the continued pendency of the captioned application.
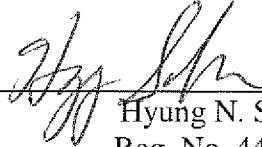
1326485

Should the Examiner feel that an interview with the undersigned would facilitate

allowance of this application, the Examiner is encouraged to contact the undersigned.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
                             Hyung N. Sohn
                             Reg. No. 44,346

HNS/edg
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

1326485